From risk management to ERM

rochette, michel

27 February 2009

From risk management to ERM

Received (in revised form): 27th February, 2009

Michel Rochette
is a professional enterprise risk manager who assists organisations to implement the main components of an ERM framework, including risk and economic capital processes, in order to create long-term value for their enterprise. Michel has been working in the risk management field since 1992 and has extensive hands-on as well as strategic risk experience. Michel's professional goal is not to sell ERM solutions to companies but to advise firms and make ethical recommendations on the best risk management practices for them. In addition to his advisory and corporate roles, Michel is also recognised as a thought leader in the ERM field, contributing innovative and pertinent presentations, articles, training and intellectual capital to the industry.

Enterprise Risk Advisory, 3838 Drolet, Montreal, Quebec H2W 2L2, Canada
Tel: +1 224 735 6466; E-mail: michel.rochette@avivausa.com; michel.rochette@enterprise-risk-advisory.com

Abstract At one point in time, there was self-insurance. Then came risk management. Now comes the era of enterprise risk management (ERM). Traditional risk management will always be necessary, but ERM will complement existing risk activities by extending the field to cover all core risks as well as emerging and strategic opportunities, because without taking risks, organisations gain no value. In addition, ERM will be taken seriously by financial participants and stakeholders if an organisation has a risk champion in the guise of a CRO, an emerging C-level position with its own set of requirements and proper training. This paper will present the main elements of an ERM framework and characteristics of different types of ERM. It will elaborate on the main roles and responsibilities of a CRO along with potential designations that would contribute to making the position fully valued and recognised by society.

Keywords: *ERM, CRO, risk management, risk designation, risk framework, risk culture, governance, risk intelligence, risk capital*

INTRODUCTION

Risk is an essential component of living. In fact, every creature on this planet must continuously evaluate the environment in which it lives, process that information, and evaluate how to adapt to changing conditions. In this way, life progresses. For example, when people moved from small country villages into larger cities during the industrial revolution, they had to adapt to a new risk environment, surrendering the capacity to make their own food. However, new opportunities emerged, and people were able to improve their standard of living due to the ensuing sophistication of exchanges.

As most people are risk-averse, they tend to focus on the negative side of risk, and forgo the opportunities represented by a well-considered risk management programme. In fact, there is nothing inherently wrong if an organisation incurs losses, as long as they are properly anticipated, managed, and the profits generated by the activities more than compensate for the losses. There is always a trade-off between risk and return.

Unfortunately, due to many external forces (mainly regulatory), most risk professionals have replicated and emphasised the negative aspect of risk-taking activities. For example, the traditional value-at-risk (VAR) measure used as the risk metric for trading portfolios is usually taken as a one-sided estimate. The credit models used to forecast credit losses only focus on the potential portfolio losses. Likewise, the methods used for operational risk again focus on the estimation of losses. In addition, these risk estimates are made in silos and never seem to embed and measure the potential for growth as afforded by involvement in core risky activities.

Thus, if the risk profession wants to continue to show its value and relevance to organisations and society at large, it should evolve and stop considering risk solely as negative, and embed the opportunities that come with risk-taking activities as well, resulting in a more balanced view. In fact, companies are looking to their risk managers' expertise and advice about emerging threats that are changing continuously, helping them turn those threats into risk-adjusted opportunities. By doing so, risk managers have the potential to become enterprise risk managers and accompany their firm into the risky 21st century. This paper will present the major tenets of this new field.

DOES RISK MANAGEMENT IN GENERAL ADD VALUE?

Before embarking on a definition of enterprise risk management (ERM), the paper will consider how risk management in general creates and sustains value.

When markets are efficient, Miller and Modigliani's financial proposition and modern financial theory suggest that investors can diversify away a firm's risk exposures — the volatility in the firm's value — by themselves very efficiently.[1] They do not need the organisation to set up a risk management framework to do so. In fact, setting up a risk management framework would destroy corporate value and reduce the value of a well-diversified investor's portfolio. Thus, equity investors should only worry about systematic risk and reflect this fact in their required rates of return as represented by the beta of the firm in the capital asset pricing model (CAPM).

However, this traditional proposition is based on a series of assumptions that have been shown not to hold in practice, particularly in a situation of financial distress. At this point, risk management shows its full relevance.

The assumption of no bankruptcy or near bankruptcy costs associated with financial distress

Contrary to this assumption, in a situation of financial distress, firms may have difficulty raising additional capital to continue their strategic expansion, resulting in under-investment and an ensuing reduction in their overall financial value. This is particularly relevant in times of severe liquidity constraints that usually accompany periods of financial distress.

Thus, if a risk management framework can allow a firm to continue to raise capital, its long-term value will be increased. Viewed from another perspective, risk management acts as a form of overall corporate

insurance — contingent capital — or as a long-term out-the-money put option that serves to eliminate or reduce the downside aspects of risk exposures while preserving the potential of upside returns. This is similar to a traditional insurance policy where one substitutes a small known loss in advance — a premium — to protect oneself against an unknown potentially devastating situation. This type of protection takes on a lot of value in times of stress, and reassures investors about the firm's value prospects.

In addition, bankruptcy costs represent a particular blow to the owners of closely-held companies, who cannot really diversify away the inherent company risks. The same situation applies to managers, employees, customers, suppliers and regulators whose situation, in many cases, is tightly aligned with the wellbeing of their company. In a firm without risk management, employees will demand higher wages and reduce their company loyalty (after all, who would want to work hard when layoffs are around the corner?), suppliers will be more hesitant to enter into long-term contracts and will be more demanding with their trade credits, and customers will be hesitant to buy the company's products because of its perceived incapacity to service them and fulfil future warranties (think of GM, Lehman Brothers and Merrill Lynch), thus decreasing the firm's value and precipitating its downfall. Risk management can alleviate those situations.

The assumption of no taxes or transaction costs

Contrary to the Miller-Modigliani proposition,[1] risk management can enhance the value of the firm by smoothing earnings and the resulting firm's tax liability through the interaction of lower marginal tax rates and tax deferrals. In addition, having a risk framework in place allows a firm to increase its debt capacity or reduce its required capital and thus benefit from the tax shield associated with the tax deductibility of the interest payments on the debt — this can be of substantial value to an organisation.

No agency conflicts within a firm

In an ideal world, all stakeholders' interests would be aligned to maximise the value of the firm. However, this is not the case in reality, particularly when stock options are granted to management and when their compensation is focused more on short-term gains than on long-term profitability. For example, managers may want to leave a firm unhedged to certain external risks with the hope of profiting through a sudden and temporary increase in the value of its corporate shares. In other cases, they may decide to pass on long-term positive net present value (NPV) projects because of their potential negative short-term impact. Thus, establishing a risk management framework with the proper limits and compensation incentives can alleviate these inherent agency conflicts by removing the selective bias created by misaligned interests within the firm.

Thus, if risk management can reduce a firm's cost of capital due to diminished potential and real bankruptcy, taxes and misaligned agency costs, it becomes a value proposition that not only smoothes reported earnings, but also enhances strategic investment decisions and value, particularly if conducted from an enterprise perspective.

ENTERPRISE RISK MANAGEMENT: A NEW PARADIGM

Beyond implementing traditional risk management frameworks, one promising avenue for risk managers to expand their role in society and in the companies in which they work is the field of enterprise risk management. Appendix A compares the main characteristics of different versions of risk management and enterprise risk management frameworks.

Traditionally, when one thinks of risk management, one thinks about the insurance specialist, broker or the auditor, who worries about the negative consequences of risk exposures. Risk is viewed in a negative way, something to avoid or to have its consequences minimised. In fact, this approach can be found in many traditional risk management standards, such as ISO and COSO I with their emphasis on controls. Other approaches are focused on risk management but solely from a compliance perspective while others focus only on overall corporate governance issues.

In recent years, risk management has been evolving into ERM. Unlike risk management *per se*, the overall goal of ERM is not simply to manage risks — particularly the expected and unexpected negative consequences that generate financial distress — but also to view risk positively, something to seek in order to create value.

However, within this broad and evolving field of ERM, there are many variations. Some aim to extend the traditional risk management approach to cover a broader set of risks and consolidate all similar exposures throughout a firm. Certain industry standards that support this approach could be characterised as enterprise-*wide* risk management. For example, standards such as COSO ERM II or AS/NZS 4360 aim to give management an assurance that, once their strategic goals are set, there will be a high probability that the firm will reach them. Enterprise risk managers are not directly involved in strategic choices but provide re-assurance.

Another version is a value-based ERM framework. A value-based ERM does not seek to replace the traditional risk management practices, which will always be necessary, but aims to integrate risk into the broader strategic decisions of the firm, identifying, measuring and managing not only the direct financial consequences of risk and opportunities but also indirect consequences like potential non-financial impact.

VALUE-BASED ENTERPRISE RISK MANAGEMENT: DEFINITION

Many definitions have been proposed in the last few years (see Appendix B). A value-based ERM (hereafter simply referred to as ERM) could be defined as the strategic enterprise process of identifying, assessing and responding to the collective risks and opportunities that may affect the enterprise's ability to attain its strategic goals, optimise its stakeholders' value and improve its overall stewardship and management. Following this approach are two recent standards, namely ISO 31000 and its European equivalent.

In addition, ERM is relevant to any organisation. An *enterprise* is more than a firm or a company, where risk management has been mostly practised

up to now. In fact, an enterprise can be described as any human organisation, whether it is for profit or not and whether it is private or public. *Risk* in this context not only includes the negative impact of risk but also the *opportunities* that any organisation should undertake in order to survive, progress and prosper. Additionally, *management* refers to the strategic decision-making processes that organisations undertake in order to manage opportunities and risks. Thus, ERM becomes an essential component of management, while a traditional risk management function — particularly a silo-based one — would be the purview of insurer brokers or some auditors, for example.

The following section will describe in more detail the main components of an ERM framework that distinguish it from other risk frameworks.

THE MAIN COMPONENTS OF ERM

The main goal of an ERM framework is to complement existing strategic management processes, allowing an enterprise to take a global, consolidated and forward-looking view of its risks and opportunities. An ERM framework should cover an enterprise's main projects, processes, products and services now and in the future, taking into account the ever-changing risk environment in which the entity operates (both external and internal), while anticipating opportunities.

In order to function properly and assist an organisation to attain its strategic objectives, an ERM framework must have a few essential components. The first two are usually found in most organisations claiming to have an ERM framework. However, to really benefit strategically from implementing an ERM approach, a few additional elements are necessary as outlined below.

First, an ERM must exist within the overall governance structure of a firm, with the proper physical, IT and human resources with well-defined roles and responsibilities, an ERM policy and standards, proper accountability and reporting relationships, and performance indicators within an overall dashboard, supported by an audit and compliance function. Secondly, the traditional risk management processes of risk ownership, reporting and treatment must be in place to execute and implement the management of the risks *per se*, particularly in the business units or in some centralised functions.

However, to be a value-based ERM framework, additional components are essential. First, there should be a risk champion, usually in the guise of a chief risk officer (CRO), who would be a C-level executive responsible for assisting the organisation with the risk aspects of its strategic choices as well as being responsible for implementing and monitoring the ERM process itself. Certain organisations appoint an overall risk manager who reports to the CFO, for instance. This is not the ideal situation as the CFO's main goal is to maximise return and then 'forget' about some of the risks in order to attain those goals. Thus, a clear separation of duties between the CFO and the CRO gives additional assurance that the risk-adjusted opportunities will be analysed and undertaken from a strategic perspective.

In fact, another essential component of an ERM framework is that the risk identification and analysis should be done from a strategic perspective, from a top-down, macro and forward-looking

view. The ERM analysis draws upon other strategic analyses such as the traditional strengths, weaknesses, opportunities and threats (SWOT) analysis and other strategic work performed by organisations. This analysis should take a broad, portfolio view, understand and model the links and correlations that may exist between different parts of the organisation and between different risks. In contrast, an ERM-wide risk framework would simply consolidate risk exposures.

In addition, an ERM framework allows an enterprise to focus its goals on the core opportunities and risks where it has a comparative advantage and to eliminate the noise created by non-essential risks. For example, for an insurer, a core risk and opportunity would be represented by demographic risks; for a banker, meanwhile, the core risk would be credit risk. Done from the strategic perspective that only an ERM value-based approach allows, a core risk then becomes the *de facto* key risk of an entity. Such a conclusion would not be reached by a traditional risk analysis. In fact, in a simple and traditional bottom-up risk analysis disconnected from the firm's strategic goals, as is often completed by less sophisticated consultants like insurer brokers, a firm could be reducing a core risk because it is perceived to have become a key risk when viewed from that perspective. However, doing so would be an inappropriate decision in the context of an ERM framework focused on value creation because it does not take into account a firm's strategic goals, financial resources and strengths at managing and generating value by assuming that core risk, which is the reason why people want to transfer the risk to that entity in the first place.

It is also essential for the chosen ERM metric to be based on a definition of value. Value should be determined from many perspectives, not just financial ones, and should be done from the perspectives of many stakeholders, not only shareholders. Indeed, private companies are usually only concerned about the financial consequences of risk, although integrating non-financial aspects can also enhance the understanding of the financial consequences of issues like corporate social responsibility, sustainability and their impact on reputation. For a governmental entity, impact might include the measurement of health and security risks and the wellbeing of its population. This approach is different from other risk frameworks such as an enterprise-wide risk framework that emphasises capital as the main metric to make decisions. Capital represents the financial resources from which a firm finances its growth and absorbs its expected and unexpected risk losses as determined from the ERM analysis.

In addition, in an ERM framework, value, risk and capital become integrated into a common framework dedicated to supporting the strategic priorities of the firm instead of being managed separately as is often the case in a silo-based risk framework. In the end, performance evaluation measures like risk-adjusted return on capital (RAROC) become the final step that links realised value created by the new opportunities and the cost of capital used to sustain those opportunities and their underlying risks. The capital structure of the firm — debt leverage versus equity — and risk management decisions thus become interchangeable so that capital affects the capacity of a firm to take on more core risks while more risk affects the capital structure of the

organisation and vice versa given its strategic goals.

Another aspect of ERM that distinguishes it from other risk frameworks is the determination of an explicit risk appetite statement — based on the same value-based metric — that will guide the organisation and the business units in their day-to-day activities through the monitoring of a limit-based risk framework. Thus, an ERM framework generates the limits instead of simply aggregating them from a bottom-up approach as would be the case in an ERM-wide or a traditional risk framework.

Finally, in a recent survey by the Economist Intelligence Unit,[2] 62 per cent of respondents mentioned that an ERM programme would be an essential component in protecting the reputation of their firm, which is another way of linking ERM with the value of the firm.

The main components of an ERM value-based framework can be summarised as follows:

- *ERM governance*:
  - board involvement and an ERM committee;
  - dedicated CRO;
  - ERM policy with well-defined roles and responsibilities;
  - independence of views sought throughout the framework;
  - complementary risk, audit and compliance functions.
- *ERM risk appetite*:
  - forward-looking financial and non-financial statement about desired risk profile translated into risk limits for all core risks.
- *ERM core risks and opportunities*:
  - identify and assess core risks and opportunities for which the firm has a comparative advantage;
  - identify, assess and prioritise in line with risk appetite and strategic objectives — risks and opportunities mapping;
  - analysis not done in silos but takes into account correlation, chain of events' potential impact, done from a top-down approach with bottom-up feedback;
  - set up processes to identify and assess emerging risks and opportunities — focus on the known unknowns as well as the unknown unknowns;
  - integrate with SWOT analysis and other strategic initiatives.
- *ERM risk assessment*:
  - determine and implement an ERM value metric — value should evaluate financial and non-financial potential impact, for example:
    - financial value metric — earnings at risk, cash flow at risk, embedded value;
    - non-financial value metric — sustainability index.
- *ERM risk intelligence*:
  - internal/external communication — inform stakeholders about risk appetite and risk/opportunities profile from a risk-adjusted value perspective;
  - implementation in day-to-day decision making with dashboards and minimum and maximum limits, not just quarterly reports to a risk committee;
  - establish continuous and forward-looking processes to identify risks and opportunities;
  - perform an overall risk and opportunities evaluation, not simply a valuation of the risks.
- *Traditional risk management processes (avoid, retain, transfer)*:

- traditional risk treatment approaches like control, hedging and insurance should be evaluated in the context of a risk-return trade-off taking into account the risk appetite;
- integrate capital and risk management as part of the risk response including contingent capital like insurance;
- establish and monitor risk limits based on a top-down view and risk appetite determination;
- establish incentives and performance measures based on the value generated by opportunities and losses anticipated;
- feedback loop — validation and back testing of the ERM processes must be implemented.

THE CHIEF RISK OFFICER: CHAMPION OF ERM

To guide an organisation towards deploying an enterprise risk management framework, more and more enterprises are creating the position of chief risk officer (CRO). The term 'CRO' was first quoted by James Lam, a well-known figure in the ERM field.[3] Like other C-level executives, this person has the responsibility to put in place a strategic enterprise risk management framework as outlined previously, and collaborate with other C-level executives during its implementation and operation.

As mentioned previously, instead of nominating a CRO, some organisations prefer to assign responsibility for ERM to another executive, namely the CFO. However, although a CFO can certainly take on these additional responsibilities, doing so entails an inherent conflict. A CFO's main responsibility is the financial wellbeing of a firm, which is certainly affected by the risks and opportunities facing the organisation. If risk evaluation is relegated to the background as the CFO's responsibilities are not primarily focused on this area of practice, there is a chance that ERM will not be part of the strategic decisions of the firm. In addition, if the CFO's remuneration is not risk-adjusted, risk evaluation might not be completed as thoroughly.

Thus, when a firm decides to appoint an independent CRO, it sends a clear signal internally and externally about its level of seriousness and commitment to carry out ERM. At this point, ERM can be integrated into the day-to-day business processes and the CRO becomes an essential partner in the growth strategies of the enterprise. Appendix C provides an overview of the main responsibilities of a CRO in an ERM context.

In addition, a CRO should develop a strategic understanding of an enterprise's core activities, especially a horizontal understanding of how a firm's processes fit together to produce the enterprise's products and services, ie its value chain. This is in sharp contrast to most risk managers' traditional silo-based view of their enterprise. They tend to be masterful at modelling and managing risks under their control with little appreciation of the relationship, correlation and impact of risks throughout the enterprise's main business activities and processes. Further, as has been demonstrated over and over, most major events that affect firms never happen in isolation but result from a chain of events, a domino effect, which can either wipe out the firm or make it very successful. Thus, the new enterprise risk manager must understand the

potential company killers in addition to helping the organisation capitalise on new risky opportunities, thus enhancing its value.

Finally, as the enterprise risk manager is not the owner of the enterprise's risks but rather an ERM facilitator, they must rely on and work with risk specialists throughout the firm, using them as their eyes and ears. Thus, interpersonal, leadership, negotiation and team-building skills are essential. In addition, excellent written and oral communication and behavioural skills adaptable to many of the different business groups within an enterprise are necessary qualities to become a successful CRO.

ERM DESIGNATIONS

So, how does one become a CRO or an enterprise risk manager? Although many gain the position through on-the-job training coupled with personal development experiences, existing risk organisations are trying to define the necessary professional training and grant designations to be recognised as an ERM expert and professional.

In spite of many recent proposals and efforts by competing risk organisations, no professional group's risk designation has yet embodied the major elements of what constitutes the essence and practice of ERM. In fact, they usually start from their existing base and try to capitalise on the emerging ERM field by adding some training that they claim will turn their members into ERM professionals. In certain cases, however, they focus too much on the quantification aspects, while in other cases they are too qualitative and replicate the traditional risk frameworks. None of them seem to be able to develop the necessary combination of quantitative, strategic and personal skills that ERM professionals must possess.

The overall goal of the enterprise risk professional designation would be to train a candidate to acquire both quantitative and qualitative skills but also ground that training in a business education context. The candidate would develop a strategic risk mindset geared towards the future and be capable of seeing the big picture, both from a risk and opportunistic perspective. In addition, a thorough knowledge of the traditional risk fields and an expertise in the dynamic nature of an industry would be necessary in order to understand and challenge existing risk techniques, particularly in financial institutions.

However, before such a potential designation takes shape, candidates for the ERM position can acquire some of the appropriate education from the existing risk organisations, the credentials of which are summarised in Appendix D. This list was compiled from those organisations that have demonstrated an interest in ERM over the last few years, both in terms of their basic training and the topics covered in their publications and during their courses and events. For some of them, membership is based on examination, while for others, it is based on experience along with some basic education.

Finally, many other organisations not listed in Appendix D offer risk designations but they are usually more focused on a particular risk or sector, and do not naturally lend themselves to the ERM-type designation. For example, risk designations such as CISA (IT/security risk), CFE (fraud risk), CPCU (casualty insurance), FLMI (life insurance), PMP (project risk) and ORPM (operational risk) do not

represent what ERM tries to accomplish, although they are essential designations in their respective fields. Enterprise risk professional training and designation would complement them, and would aim to work alongside them but from a strategic and top-down perspective.

CONCLUSION: RISK CULTURE

ERM represents an opportunity for traditional risk managers to take on a more strategic role, and assist their enterprise to create value while integrating all core risks and opportunities, both existing and emerging. However, without a strong risk culture for the CRO to develop and nurture, the chance of success will be limited. In fact, an organisation that is continuously in a crisis mode and reacting to events is not in a risk management mode, let alone an enterprise risk mode, where it can anticipate and position itself accordingly.

In fact, an organisation that has a strong risk culture is one that is forward-looking, has taken a strategic approach to risk and opportunities and embedded it throughout the organisation. In addition, building a strong risk culture implies that an enterprise is willing to learn from its mistakes and is sufficiently agile to respond to emerging threats and opportunities, not just wait for things to happen and improve continuously, allowing it to optimise its value.

Finally, developing a risk culture that can sustain ERM takes time and a continuous commitment by the organisation. The tone must be set from the top, yet the organisation's people must have a sense of ownership and accountability. There must also be a great deal of transparency, and excellent communication by ERM's primary champion, the CRO.

References

1 Modigliani, F. and Miller, M. H. (1958) 'The cost of capital, corporate finance and the theory of investment', *American Economic Review*, Vol. 48, No. 3, pp. 261–297.
2 Economist Intelligence Unit (2008) 'The Bigger Picture: Enterprise Risk Management in Financial Services Organizations', SAS and EIU, p. 6.
3 Lam, J. (2003) 'Enterprise Risk Management: From Incentives to Controls', Wiley Finance.
4 Arthur Andersen (2000) 'Enterprise-Wide Risk Management: Strategies for Linking Risk and Opportunity', Arthur Andersen.
5 Casualty Actuarial Society (2003) 'Overview of Enterprise Risk Management', Enterprise Risk Management Committee.
6 AIRMIC, IRM, ALARM (2002) 'A Risk Management Standard', FERMA.
7 Risk and Insurance Management Society (2008) 'State of ERM 2008 Report', RIMS.
8 Liebenberg, A. and Hoyt, R., Terry College of Business, University of Georgia (2003) 'The Determinants of Enterprise Risk Management: Evidence from the Appointment of Chief Risk Officers', *Risk Management and Insurance Review*, Vol. 6, February, pp. 37–52.
9 Shimpi, P. A., Towers Perrin (2001) 'Integrating Corporate Risk Management', Texere.

Further reading

Apgar, D. (2006) 'Risk Intelligence: Learning to Manage What We Don't Know', Harvard Business School Press, Boston, MA.

Barton, T. (2001) 'Making Enterprise Risk Management Pay Off', Financial Executives Research Foundation.

Chapman, R. J. (2006) 'Simple Tools and Techniques for Enterprise Risk Management', Wiley Finance Series.
Chew, D. H. (2008) 'Corporate risk management', *Journal of Applied Corporate Finance*.
DeLoach, J. W. (2000) 'Enterprise-Wide Risk Management', Financial Times-Prentice Hall, London.
Doff, R. (2007) 'Risk Management for Insurers, Risk Control, Economic Capital and Solvency II', Risk Books.
Merton, R. C. (2005) 'You have more capital than you think', *Harvard Business Review*, Vol. 83, No. 11, pp. 84–94.
Moeller, R. R. (2007) 'COSO ERM: Understanding the New Integrated ERM Framework', John Wiley & Sons.
Monahan, G. (2008) 'Enterprise Risk Management: A Methodology for Achieving Strategic Objectives', John Wiley & Sons.

APPENDIX A: THE MAIN CHARACTERISTICS OF RISK MANAGEMENT FRAMEWORKS

- Control (silo-based) risk frameworks:
  - cover a subset of risks including insurance, hazard, financial and operational;
  - conduct risk management in silos;
  - focus on the negative side of risks;
  - mitigate risk through financial and operational controls and insurance coverage, such as:
    - ISO standards;
    - COSO I, COCO for accounting;
    - COBIT for IT risk;
    - PRINCE for project management;
    - actuarial control cycle for insurance products;
    - BS 25999 (business continuity);
    - ISA 400, SAS 70 for controls evaluation of service organisations;
    - quality management approaches to reduce error rates;
    - IFC performance standards on social and environmental sustainability, such as the Equator principles on social and environmental risks.
- Compliance and regulatory risk frameworks:
  - focus on conformity to laws, rules, regulations and internal policies;
  - used to focus only on compliance but have recently shifted to more risk-based compliance; examples include:
    - SOX, JSOX, anti-money laundering policy;
    - Basel II pillar I (focused on solo risk measurement through capital estimation, ICA);
    - Solvency II Pillar I (a compliance exercise but with a wider set of risks);
    - Turnbull Report on Internal Controls;
    - NAIC Risk-Based Framework;
    - UK FSA Organizational Systems and Controls;
    - Europe MIFID.

- Governance frameworks:
  - — focus on high-level principles of governance by organisations;
  - — establish roles, responsibilities and delegation of authorities to support ERM; examples include:
    - NYSE governance standards;
    - the UK Cadbury Report;
    - GRC — attempts to streamline governance, risk and compliance functions;
    - recent framework proposals by the hedge fund and asset management communities.
- Enterprise-wide risk (integrated/capital based) management frameworks (bottom-up):
  - — extend risk management to take a consolidated view of existing risks and assess additional risks like liquidity, business and strategic, reputational, environmental, social responsibility; examples include:
    - COSO ERM II;
    - AS/NZS 4360;
    - CAN/CSA-Q850;
    - Moody's RMA, Fitch risk model and AM Best's ERM;
    - Basel II/Solvency II Pillars II and III (extend the pure compliance aspect to a wider ERM framework and ORSA for solvency II).
- Enterprise risk management (holistic/value-based) frameworks (top-down):
  - — ISO 31000;
  - — Europe Risk Management Standard by FERMA, ALARM, AIRMIC, IRM;
  - — Standard & Poor's ERM for Financial Institutions;
  - — RIMS Risk Maturity Framework.

APPENDIX B: SOME ERM VALUE-BASED DEFINITIONS

- *Former Arthur Andersen* 'A structured and disciplined approach that aligns strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties the enterprise faces as it creates value . . . It is truly holistic, integrated, forward-looking . . . of managing all key business risks and opportunities with the intent of maximizing shareholder value.'[4]
- *The Casualty Actuarial Society (CAS)*: 'ERM is a discipline by which an organization in any industry assesses, controls, exploits, finances and monitors risks from all sources for the purpose of increasing the organization's short and long-term value to its stakeholders.'[5]
- *A Risk Management Standard by the Federation of European Risk Management Associations (FERMA), AIRMIC, ALARM, IRM*: 'Risk Management is a central part of any organization's strategic management . . . It is a process whereby organizations methodically address the risks attached to their activities with the goal of achieving sustained benefit . . . and understanding the potential downside and upside of all the factors which can affect the organization.'[6]
- *Risk and Insurance Management Society (RIMS)*: 'ERM is the culture, processes, and tools to identify strategic opportunities and reduce uncertainty. It is a comprehensive view of risk both from operational and strategic perspectives and is a process that supports the reduction of uncertainty and promotes the exploitation of opportunities.'[7] (Although not explicitly stated, value creation is implied in this definition and in the standard.)

- *Center for Strategic Risk Management, University of Georgia's Terry College of Business*: 'ERM is a corporate wide, as opposed to departmentalized, effort to manage all the firm's risks — in fact, its total liability structure — in a way that helps management carry out its goal of maximizing the value of the firms' assets.'[8]
- *Towers Perrin*: 'A rigorous approach to assessing and addressing the risks from all sources that threaten the achievement of an organization's strategic objectives. In addition, ERM integrates those risks that represent corresponding opportunities to exploit for competitive advantage.'[9]

APPENDIX C: A JOB DESCRIPTION FOR A CRO

Develop, maintain and evolve a value-based ERM framework that serves to identify, assess and manage all core risks and opportunities that are in line with the enterprise strategic goals, values, culture and risk appetite.

- Establish and update the appropriate ERM governance framework, proper roles and responsibilities, and policies.
- Develop, communicate and monitor — dashboard — the risk appetite statement of the organisation.
- Establish an appropriate compensation programme that links value, risks and performance incentives.
- Actively participate in the strategic decisions of the organisation, bringing that risk/opportunity perspective in initiatives like new markets, products and services, mergers and acquisitions, annual planning etc.
- Develop expertise in ERM processes for core risks and opportunities and their potential impact on reputation and value: identification, evaluation, measurement and management of core risks, SWOT analysis, correlations and horizontal view of risks — value chain — in products and services, IT, HR, financial and operational risk processes, risk controls, corporate insurance, risk monitoring (IT system), risk resilience (business continuity) and compliance.
- Develop and implement appropriate risk intelligence processes to anticipate emerging risks and opportunities (especially unexpected situations) by evaluating the potential impact on the value of the firm, both from financial and non-financial risks — known unknowns and unknown unknowns.
- Develop the appropriate value metric (eg financial, like earnings-at-risk and cash flow-at-risk, and non-financial, like sustainability index) that fits with the strategic goals of the organisation, its culture and its environment along with other metrics like Balanced Scorecard, KPIs, KRIs.
- Align risk management and capital structure decisions: economic capital, capital budgeting decisions, cost/benefit analysis of newer risk management activities, capital allocation to business units.
- Reassess the ERM framework in light of company and external development and audit recommendations.
- Be the primary liaison on ERM issues with external parties: regulators, rating agencies and the financial community.

APPENDIX D: SUMMARY OF POTENTIAL ERM DESIGNATIONS AND THEIR SPONSORING ORGANISATIONS

Organisation	Credential	Comments
Global Association of Risk Professionals (GARP)	Financial Risk Manager (FRM) & Associate (November 2009)	Mostly large international banks/ investment management firms Mostly focused on financial risks Agreements with universities to train their FRM candidates Specialised certificates in energy, banking and regulation, risk in Islamic financial institutions
Professional Risk Managers' International Association (PRMIA)	Professional Risk Manager (PRM)	Focus on financial institutions like banks, asset managers and insurance companies Focus on financial, operational and strategic risks Agreements with universities to train the PRM candidates New Associate PRM designation PRMIA Institute is their continuing education arm Co-sponsor of the annual ERM symposium
Actuarial organisations		
— Society of Actuaries (SOA)	Chartered Enterprise Risk Analyst (CERA) in addition to its FSA designation	Mostly focused on the insurance/ pension industries Highly focused on the quantitative aspect of certain risks Main sponsor of the annual ERM symposium with CAS
— Casualty Actuarial Society (CAS)	No risk designation *per se* but its FCAS	Work with ERM II to develop links with universities
— Canadian Institute of Actuaries (CIA)	No risk designation *per se* but its FCIA/FICA	Co-sponsor of the ERM symposium and other risk projects
— International Actuarial Association (IAA)	Development of an international ERM designation	Global association of actuarial organisations which supports the profession worldwide Each country has admission standards, continuing education requirements, standards of practice, disciplinary processes
Americas		
— Risk and Insurance Management Society (RIMS)	RIMS Fellow for experienced risk professional Issued in conjunction with these basic risk management designations: Associate in Risk Management (ARM); Canadian Risk Management (CRM)	Traditional insurance risk and risk finance professionals in all industries with a high concentration in the corporate sector Basic designations highly focused on the traditional risk management process RIMS has taken on ERM as one of its newer sectors

Continued

Continued

Organisation	Credential	Comments
— National Alliance for Insurance Education and Research	Certified Risk Manager (CRM)	
— ALARYS for South America	Alarys International Risk Manager (AIRM)	
Australia/NZ		
— Risk Management Institution of Australasia (RMIA)	Certified Practicing Risk Manager (CPRM) Certified Risk Management Technician (CRMT)	RMIA is the author of the AS/NZS 4360 Risk Management Standard
Asia		
— Asian Risk Management Institute (ARiMI)	Enterprise Risk Manager (ERM) Certified Professional Risk Manager (CPRM) Fellow in Applied Risk Management (FARM)	Done in collaboration with the university of Singapore Based in insurance but with extension to ERM topics
Europe		
— Federation of European Risk Management Associations (FERMA)	A pyramid of risk designations from the Diploma and Certificate to Fellowship issued by the Institute of Risk Management (IRM)	FERMA is an organisation of European risk organisations dedicated to the wide-ranging risk interests of its members, both from the public and private sectors Promotes the use of the Risk Management Standard
— Association of Insurance and Risk Managers (AIRMIC in the UK)		Insurance managers but with an interest in ERM development and implementation
Public sector risk management associations		
— PRIMA/PARMA in North America — ALARM in the UK	No designation *per se*	Associations dedicated to the risk management needs of the public sector in the USA/UK
University-based risk education		
— Business schools — Actuarial schools — Financial engineering schools — Risk management schools	MBA/master/PhD degrees in insurance and risk management	Many offer some ERM-focused courses along with their association with professional risk organisations Some are offering ERM type courses as well; for example Stanford University Certificate in Strategic Risk Management and Master Certificate in ERM by CBET at the University of Waterloo